Before the
Public Safety and Homeland Security Bureau
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	PS Docket No. 10-146
A Cybersecurity Roadmap	)	GN Docket No. 09-51
	)	

PUBLIC COMMENT

COMMENTS OF YAANA TECHNOLOGIES, LLC

Anthony M. Rutkowski
SVP for Regulatory Affairs and Standards
Yaana Technologies, LLC
500 Yosemite Drive, Suite 120
Milpitas, CA 95035
tel: +1 408.854.8041
mailto:tony@yaanatech.com

Raj Puri
CEO
Yaana Technologies, LLC
500 Yosemite Drive, Suite 120
Milpitas, CA 95035
tel: +1 408.854.8030
mailto:raj@yaanatech.com

Filed: 23 Sep 2010

1. Yaana Technologies (Yaana) is a Silicon Valley based company focused globally on providing unique and high-value Managed Services to enterprises and networked communications service providers that include identity management, cyber security and forensic compliance capabilities for service providers, including Trusted Third Party implementations. In the course of these activities, Yaana principals have participated for many years in numerous domestic and international technical and policy forums dealing with cyber security. Mr. Rutkowski presently is the appointed Rapporteur for Cybersecurity in the principal global intergovernmental/industry venue for technical cyber security matters, the Geneva-based International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) as well as the Rapporteur for the global eWarrant technical specification in the European Telecommunication Standardization Institute (ETSI), but not commenting in either of those capacities in this proceeding. In particular, he has led representatives from nations throughout the world in a similar cybersecurity roadmap development and implementation process.

2. In its 9 August *Public Comment Notice*, Public Safety and Homeland Security Bureau (PSHSB) sought public comment on the creation of a Cybersecurity Roadmap to identify vulnerabilities to communications networks or end-users and to develop countermeasures and solutions in preparation for, and response to, cyber threats and attacks in coordination with federal partners. Yaana has already provided relevant *ex parte* briefings and comments related to cybersecurity in this and other related proceedings in the United States and other countries, and welcomes the opportunity to address the numerous specific questions in this public notice comment process.

A. The Commission's Cybersecurity Roadmap must be international in scope

3. Almost every nation on earth is undertaking the establishment of a similar cybersecurity roadmap, and most are seeking to do so in collaboration with their counterparts through a variety of bilateral and multilateral mechanisms. The existence of common global platforms that execute the same software and malware, and are susceptible to the same kinds of vulnerabilities and attacks, compels cooperative

worldwide approaches. In addition, no one nation or organization possesses definitive wisdom, and collective collaboration seems appropriate; and in many cases, the roadmaps and actions being taken by other national regulators can be viewed as implementations to be evaluated by the Commission for effectiveness.

4. The international scope of the cybersecurity challenges has produced a complex and constantly evolving ecosystem of organizational actors and strategies in play – each with its own benefits, detriments, and limitations. The environment and its evolution bears strong resemblance to the appearance of the last great global open network infrastructure – the radio-based wireless internet of 100 years ago. Then as now, years of dialogue ensued concerning the relative merits of governmental and intergovernmental actions and the potential adverse effects on innovation and roles of the private sector in the face of ever worsening attacks and detriment to the communications infrastructure. Ultimately sets of flexible effective legal, technical, and enforcement mechanisms were developed, applied, and evolved among and within the world's nations.

5. The roadmap approach described below is a product of a subset of domestic and international activities that has encompassed industry, academic, and government agencies in the national security information assurance, incident response, and enforcement communities. Although it is certainly not the only roadmap, it does have the benefit of some longevity, broad global vetting and buy-in, and contributions from significant trusted expert communities. The details of the roadmap constantly evolve.

B. The Commission's Cybersecurity Roadmap should begin with an accepted global generic model for what constitutes cybersecurity

6. Although threads of global cybersecurity collaboration have their antecedents over about sixteen decades, the contemporary focus largely emerged from U.S. government funded work facilitated by the legendary Dr. Prescott B. Winter and occurring under the aegis of the Stanford University's CRISP (Consortium for Research on Information Security and Policy) initiative in the late 1990s, and led in large measure by DARPA Director Emeritus Dr. Stephen J. Lukasik with Dr. Seymour E. Goodman.

Both have enjoyed extensive prominent careers in the national security scientific community. Dr. Lukasik is notable, among other things, for being the Director under whom the TCP/IP protocol was developed, as well as instrumental within multiple high level U.S. government strategic policy positions including serving as the FCC's first Chief Scientist and chief of its Office of Science and Technology.[1]

7. In 2007 as the U.S. domestic and global cybersecurity dialogue ramped up, the Georgia Institute of Technology (GeorgiaTech) hosted an international cybersecurity conference that resulted in Lukasik, Goodman, and Rutkowski preparing and evolving a diagrammatic model for what constitutes cybersecurity. Georgia Tech also hosted the President's National Security Telecommunications Advisory Committee (NSTAC) Research and Development Conferences at which cybersecurity was an emerging concern. This cybersecurity depiction was undertaken because it became apparent at the time that countless different conceptualizations of cybersecurity existed among different individuals and groups. If any meaningful comprehensive treatment of cybersecurity is to ensue, it is essential that the involved parties have the same understanding of what they were dealing with.

8. Figure 1, below, is the present stable depiction of the original Georgia Tech cybersecurity model that has been subsequently introduced, evolved, and accepted in multiple diverse international venues, including the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) and the European Network and Information Security Agency (ENISA). The original model included an elaboration of the different connotations of security that was subsequently truncated to portray only actionable components. The model begins with five clusters of cybersecurity purposes in a clockwise order: measures for protection, measures for threat detection, investigation and countermeasure initiation – that include thwarting and other remedies, including legal measures. At a more detailed level, each cluster includes several specific capabilities that are interrelated by flows of information that enable cybersecurity actions to take place.

9. A broad consensus on this cybersecurity model has subsequently facilitated useful global collaboration on the existence, adequacy, and implementation of specific

[1] At the time, Yaana SVP Rutkowski was a staff advisor to Dr. Lukasik at the FCC.

capabilities. The Commission's Cybersecurity Roadmap should begin with such an accepted global generic model for what constitutes cybersecurity. Indeed, it is not apparent that any meaningful roadmap could exist without a common understanding of what constitutes cybersecurity.

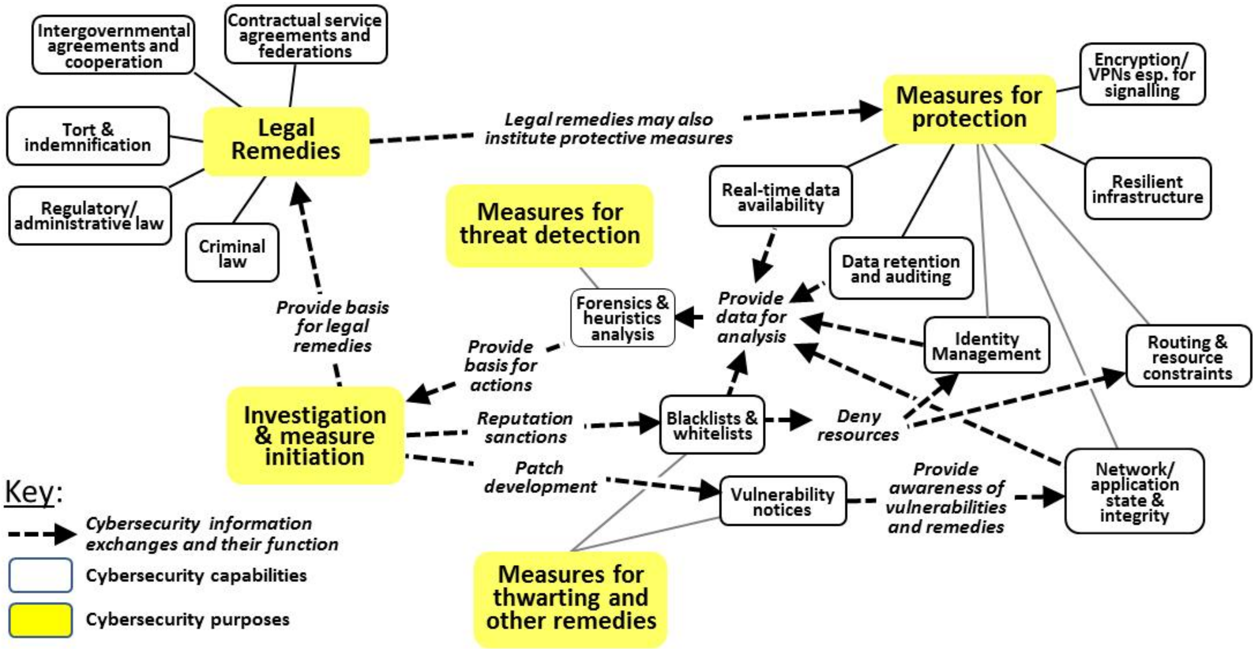
Intergovernmental agreements and cooperation
Contractual service agreements and federations
Tort & indemnification
Legal Remedies
Regulatory/ administrative law
Criminal law
Legal remedies may also institute protective measures
Measures for protection
Encryption/ VPNs esp. for signalling
Resilient infrastructure
Real-time data availability
Data retention and auditing
Measures for threat detection
Forensics & heuristics analysis
Provide data for analysis
Identity Management
Routing & resource constraints
Provide basis for legal remedies
Provide basis for actions
Investigation & measure initiation
Reputation sanctions
Blacklists & whitelists
Deny resources
Patch development
Vulnerability notices
Provide awareness of vulnerabilities and remedies
Network/ application state & integrity
Measures for thwarting and other remedies
Key:
Cybersecurity information exchanges and their function
Cybersecurity capabilities
Cybersecurity purposes

Figure 1 - Global Cybersecurity Model

C. The Commission's Cybersecurity Roadmap should include the frameworks for capabilities necessary to implement the model

10. Following the development of a model for what constitutes cybersecurity, the Commission's roadmap can then consider how to bring about the various capabilities of the model – recognizing its national jurisdiction and resources to do so on the requisite scale. Massive cooperation is required. There are, however, capabilities that are more readily addressed than others, and Figure 2, below, is designed to depict sets of capabilities that have synergistic relationships and worth special focus as being implementable through concerted government-industry action domestically and internationally. Indeed, some of these actionable areas have been used particularly effectively over many decades both under radio regulatory regimes established by the Commission, as well as CALEA requirements for enabling the availability of law

enforcement forensics. The general thrust here is that identity management of service/software providers, users and objects are essential assurance mechanisms that operate in concert with mechanisms for system integrity, incident forensics, and law enforcement forensics.

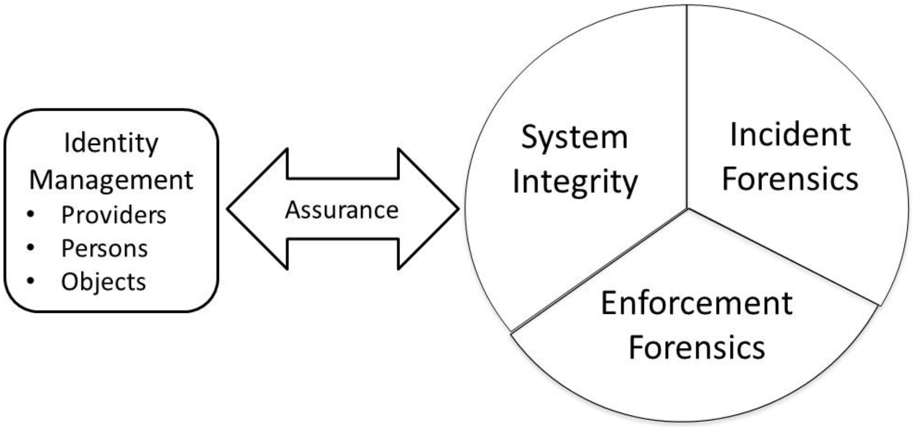

Figure 2 – Principal areas of focus for roadmap implementation

11. Following many months of considering what actions could be taken to implement its cybersecurity roadmap, the ITU-T pursued the development of a major initiative to identify and adopt within a comprehensive framework, the available best-of-breed standardized platforms for enabling the trusted exchange of cybersecurity information to achieve many of the essential capabilities in Fig. 2, above. The result at a high level is depicted in Fig. 3, below, and set forth in substantial detail in a new draft standard designated Recommendation ITU-T X.cybex, *The Cybersecurity Information Exchange Framework*. The framework mirrors and expands upon a similar one pursed by the government information assurance agencies in more than a dozen nations under the aegis of the Common Criteria Control Board. These frameworks draw upon proven techniques in widespread use that rely on common sense needs: know who and what you are dealing with, make security measureable to maximize the integrity of platforms you are using, watch for incidents, and when they occur, take appropriate action to share the information within a trusted community for action against the perpetrators. Whether it is a network infrastructure, radio spectrum use, or physical security of premises, these are essential steps to be taken.

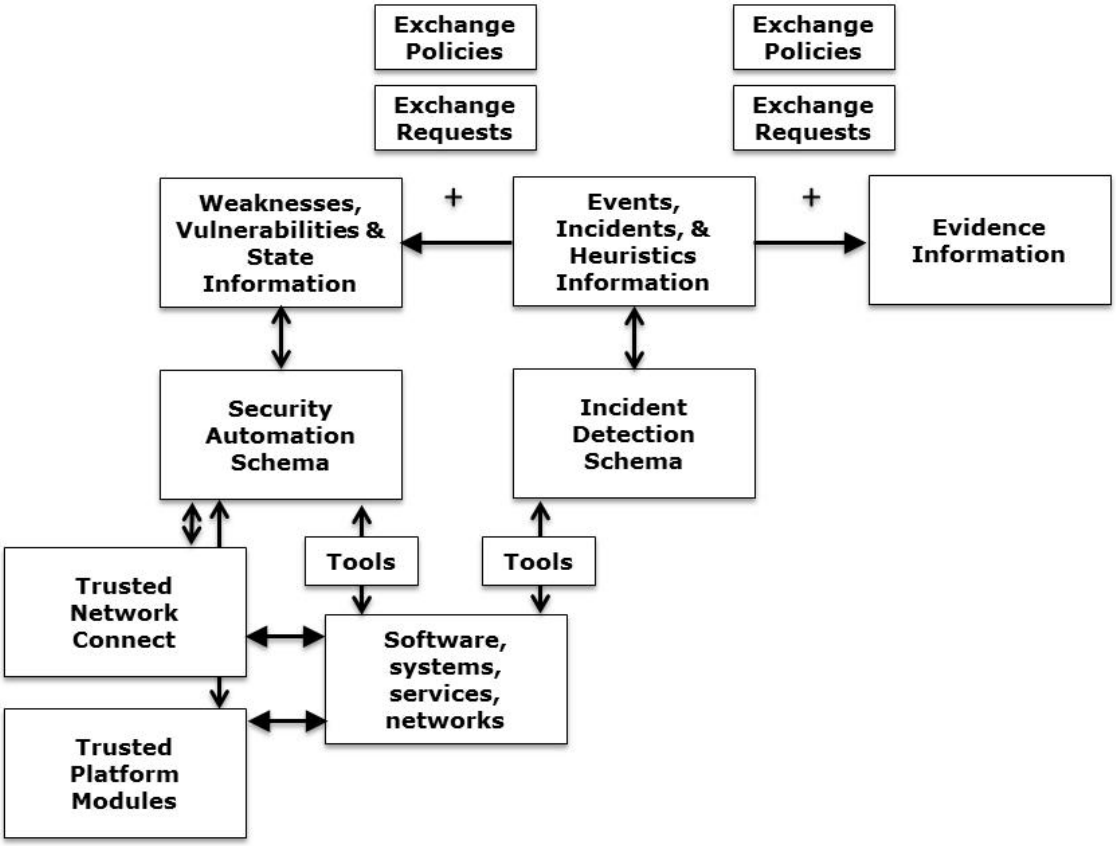
Exchange Policies
Exchange Requests
Exchange Policies
Exchange Requests
Weaknesses, Vulnerabilities & State Information
+
Events, Incidents, & Heuristics Information
+
Evidence Information
Security Automation Schema
Incident Detection Schema
Tools
Tools
Trusted Network Connect
Software, systems, services, networks
Trusted Platform Modules

Figure 3 – Operational Capabilities Necessary for Cyber Security

D. The Commission's Cybersecurity Roadmap should include the mandates and cooperative activities necessary to bring about the framework capabilities

12. The most difficult parts of any Commission cybersecurity framework revolve around finding the requisite resources to discover and engage in the enormous number of cooperative activities that exist today, as well as instituting mandates or otherwise facilitating necessary actions. There is a long history of doing so in the radio domain; but much less so for network infrastructure. Additionally, the past twenty years of substantial abandonment of a significant network infrastructure security role to voluntary private sector action by the Commission will be difficult to overcome. Even when the needs are essential - such as for CALEA and Cybercrime Convention based IP network

cybersecurity forensics - the actual implementation of even minor requirements as Commission rules remain unanswered.[2]

13. The Commission has ample jurisdiction under an array of domestic statutory and international treaty instruments to implement cybersecurity mandates as part of its roadmap. Some actions such as the ubiquitous mandated deployment of and support for stable proven capabilities such as the Extended Validation Certificate provider identity management platform would produce significant immediate cybersecurity benefits. Other capabilities pioneered by the government information assurance community such as trusted computing and secure automated integrity platforms are also in this category. It seems essential for the Commission as part of its roadmap to explicitly provide for the potential instantiation of identified cybersecurity capabilities in the form of regulatory mandates or equivalent, lest the roadmap remain an academic exercise.

[2] U.S. Dept. of Justice, Petition for Expedited Rulemaking to Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act, 15 May 2007.